ADVANCED CELL PHONE FORENSICS CONFERENCE

February 8, 2019
APAAC Training Room
Phoenix, Arizona

CELLEBRITE AND THE DIFFICULTY OF GETTING INTO PHONES FOR EVIDENCE EXTRACTION

Presented by:

Katherine Enriquez
Detective, Maricopa County Attorney's Office

Distributed by:

ARIZONA PROSECUTING ATTORNEYS' ADVISORY COUNCIL
1951 West Camelback Road, Suite 202
Phoenix, Arizona 85015

ELIZABETH ORTIZ
EXECUTIVE DIRECTOR

Cellebrite and the difficulty of getting in to phones

Detective Kathy Enriquez
Maricopa County Attorney's Office
Investigations Division

1

CELLEBRITE

- Most popular of all forensic extraction software, most well known (but it is not the only one out there)
- Founded in 1999 in Petah Tikva, Israel
- Owned by Sun Corporation out of Japan
- Headquartered in Israel
- Has offices in New Jersey, Florida and Washington
- Initially created for a phone to phone transfer of data by telecom companies when a new phone was purchased
- 2007 introduced "Universal Forensic Extraction Device (UFED)

2

Cellebrite

- UFED is sold only to approved government and corporate organizations (insert defense experts here)
- Ability to break codes, decipher encrypted information and acquire hidden and deleted data
- Supports over 10,000 devices including cell phones, tablets, GPS units, drones
- Supports both CDMA and GSM technology
- Interfaces with operating systems such as iOS, Android OS, BlackBerry, Symbian, windows Mobile and Palm

3

Type of Extractions

- Manual: Scrolling through the device and taking photographs of the screens. Very time consuming but necessary in some cases
- Logical: "what you see is what you get". If you can see it while scrolling through the device, it should extract the information
- File System: extracts the directories and files
- Physical: a bit for bit copy of the mobile device's entire storage including recovering deleted information, deciphering encrypted data and acquiring information from password-protected applications

4

What happens when Cellebrite doesn't work

- Chip Off: an advanced digital data extraction and analysis technique which involves physically removing the flash memory chip from the device with heat or cold and then using software to make a copy of the information on the memory chip. That image/copy can then be loaded in to Cellebrite or other forensic software to read the information.
- JTAG: an advanced level data acquisition method which involves attaching electrodes directly to the data memory chip to extract a full physical image of the information on the memory chip.
  - Both methods required additional training by the examiner and are very expensive

5

What happens when none of those methods work?

- More and more devices are being released with "built in" encryption mechanisms including iPhone and Android
  - Since 2015 Android devices have default full disk encryption
  - The Encryption was software based
  - The use of "brute force techniques" could still be used to attempt multiple passcodes repeatedly until the content was successfully decrypted.
    - System does not recognize the attempts and does not destroy data

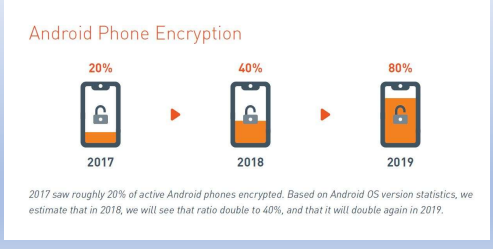
6

Hardware Based Encryption

- Once the manufacturers discovered forensic software and Law Enforcement had "broken" they software based encryption, they created Hardware Back Encryption effectively "closing" the back door discovered.
- For the past three (3) years Apple and Android devices have been sold with hardware backed encryption.
- The ability to decrypt the information contained in the device, is built in to the hardware of the device. Without the "key", the device will not decrypt the data even if an extraction could be performed.
- Eliminated both JTAG and Chip Off capabilities

7

Number of Encrypted Android Phones



8

•Where does this leave us?

9

Apple Devices / Gray Key

10

Android

- The best solution currently for locked/encrypted Android phones is to send the device to Cellebrite who will provide a physical copy of the device.
- The FBI is currently in the testing process for a technique they developed and should be able to assist in the near future
- Lockdown pList

11

Other Forensic Tools:

- Oxygen Forensic Suite
- Secure View
- XRY

12

- Lets go through a UFED report

13

Detective Kathy Enriquez
Maricopa County Attorney's Office
enriquek@mcao.Maricopa.gov
602-448-3968 cell phone
602-372-6991 desk phone

14